IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF OHIO

IN THE MATTER OF THE SEARCH OF THE PROPERTY OF WILLIAM KISOR, LOCATED AT 25630 CANAL RD., CIRCLEVILLE, OH 43113, FURTHER DETAILED IN ATTACHMENT A, INCORPORATED HEREIN BY REFERENCE	Case No. 2:25-mj-6 **Filed Under Seal**

AFFIDAVIT IN SUPPORT

I, Edward A. La Vigne, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I have been employed as a Special Agent of the U.S. Department of Homeland Security, Homeland Security Investigations ("HSI"), since 2010, and am currently assigned to HSI Columbus, OH. While employed by HSI, I have investigated federal criminal violations related to technology or cybercrime, child exploitation, and child pornography. I have gained experience through training at the Federal Law Enforcement Training Center (FLETC) and everyday work relating to these types of investigations. I have received training in the area of child pornography and child exploitation and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256(8)(A)) in all forms of media including computer media. Moreover, I am a federal law enforcement officer who is engaged in enforcing the criminal laws, including 18 U.S.C. §§ 2251, 2252, and 2252A, and I am authorized by law to request a search.

2. This Affidavit is submitted in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant for the residence of William KISOR, located at 25630 Canal Rd., Circleville, Ohio, within the Southern District of Ohio ("SUBJECT PREMISES") more fully described in Attachment A for electronic storage devices, and to search said devices for

contraband and evidence, fruits, and instrumentalities of violations or attempted violations of 18 U.S.C. §§ 2422 and 2252A, which is more specifically described in Attachment B of this Affidavit.

3. The statements contained in this affidavit are based in part on information provided by U.S. federal law enforcement agents; written reports about this and other investigations that I have received, directly or indirectly, from other law enforcement agents; information gathered from the service of administrative subpoenas; the results of physical and electronic surveillance conducted by law enforcement agents; independent investigation and analysis by law enforcement agents/analysts and computer forensic professionals; and my experience, training and background as a Special Agent. Since this Affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that contraband and evidence, fruits, and instrumentalities of violations or attempted violations of 18 U.S.C. § 2422(b) (attempted enticement of a minor to engage in illicit sexual activity); and 18 U.S.C. § 2252A (distribution, receipt and possession of child pornography) are within electronic storage devices located at the SUBJECT PREMISES.

PROBABLE CAUSE

4. In January of 2023, a Homeland Security Investigations (HSI) Colorado Springs undercover Special Agent (herein referred to as "the UC") acted in an undercover capacity online a mobile messaging application (hereinafter the "App") to detect and investigate violations of federal law related to the sexual exploitation of children. The UC's assumed the persona of an adult mother with a 23-year-old daughter, 15-year-old daughter, and 8-year-old twin daughters, herein referred to as "Child 1" (23), "Child 2" (15), "Child 3" (8), and "Child 4" (8). The UC had previously been in contact with KISOR prior to his 135-month incarceration for 18 USC 2252,

(a)(4)(b) – possession of Visual Depictions of Child Pornography. KISOR was convicted and sentenced in the Southern District of Ohio in case #2:12-cr-00141. After KISOR's release from prison, he (KISOR) resumed his contact with the UC, never realizing she was an agent of law enforcement.

5. On January 26, 2023, KISOR contacted the UC via email in an attempt to reengage the UC. Prior to his incarceration, KISOR believed he and the UC would enter into an incestuous relationship involving her notional daughters, "Child 1," at the time aged 14, and "Child 2," at the time aged 4. The UC received an email from KISOR via Yahoo account wrk1968@yahoo.com, the same email account KISOR used in 2012 to communicate with the UC. KISOR referenced the UC's persona name, along with the persona names of "Child 1" and "Child 2." KISOR also shared a picture with the UC he had saved to his email account from 2012. The picture was of the UC's notional "Child 1." In the new emails from KISOR, he provided his phone number (614-753-6570) to the UC so they could begin text messaging. KISOR and the UC then began communicating again, with the UC posing as the aforementioned mother and each of the children.

6. KISOR asked the UC via email if she was currently "active" with anyone, your affiant knows the term "active" is used to refer to a physical relationship between individuals. The UC answered KISOR, saying she was not currently in a relationship at that time. On February 6, 2023, KISOR and the UC exchanged several email communications. The UC shared her skepticism that the individual communicating with her was KISOR. KISOR then provided several details to the UC to affirm it was in fact him (KISOR) emailing her (UC). On February 28, 2023, KISOR reaffirmed his desire to initiate an incestuous relationship with the UC and her notional children. The UC had previously disclosed to KISOR that she now had eight (8) year old twins since they last communicated, in addition to her now adult daughter (age 23) and daughter (age

14). During the communications on this date, KISOR believed he was texting with "Child 2" and "Child 3" and shared his desire to be their "first" referring to sexual encounter/partner. At the time, KISOR believed "Child 2" to be 14 years old, and "Child 3" to be 8 years old. As outlined below, in follow up text messages between KISOR, the UC and her notional children, he shared his desire to perform various sexual acts with the UC and her children. KISOR was extremely descriptive and graphic when describing the acts he'd like to perform on them and he would like them to perform on him.

7. During these communications, KISOR also texted with the UC posing as "Child 1," who would now be an adult. On February 17, 2023, KISOR texted "Child 1" and asked if she remembered the "special toy" he showed her back in 2012, when "Child 1" would have been 14 years old. KISOR, believing he was texting with Child1 stated he would be "their first" "but only if they want to," referring to "Child 3" and "Child 4." Throughout the course of these text messages, KISOR repeatedly asked the UC if she could send him pictures of her daughters and expressed his desire to not only be in a sexual relationship with the UC and her daughters, but to also be their "daddy."

8. On February 24, 2023, KISOR sent the UC two photos of himself via text message. In the first photo, KISOR is seen wearing black rimmed glasses and a blue long-sleeved shirt. In the second photo, KISOR is seen wearing a gray t-shirt and standing in a room with metal bunk beds behind him. According to the UC, the photos sent by KISOR match or are like previous photographs the UC has seen of KISOR.

9. During a text exchange on March 2, 2023, the UC asked KISOR how their relationship would work if he could not leave the state of Ohio for 10 years due to his supervision and KISOR replied that one of them would have to move. The UC went on to ask KISOR, "are

you even allowed to be around kids for ten years or would that violate your parole?" KISOR replied "I can be around kids with supervision" and "it wouldn't violate me." The UC replied "so they could never find you alone with the girls. Could they live there?" KISOR then responded "Yes, especially after we would get married," followed up with him saying "I would be their step-father."

10. On March 3, 2023, KISOR texted with the UC posing as "Child 4." KISOR asked about "Child 3." "Child 4" eventually told KISOR "Momma told us about you wanting to be daddy." KISOR stated "Doesn't ['Child 3'] want to meet me?" "Child 4" responded "Yeah, but she is like super shy all the time." KISOR then told "Child 4" "I would love very much to be your dad." "Child 4" stated "she says our daddy has to be a special kind of daddy, not like other daddies." KISOR asked "Child 4" "what kind of daddy would that be?" "Child 4" responded "a daddy that sleeps with us all the time. And does special stuff." The UC later sent an image via text of twin girls to KISOR.

11. On or about March 13, 2023, KISOR texted the UC and asked, "So tell me: How good does she taste?" The UC responded "'Child 3' or the twins. All sweet but that's for later." KISOR then stated, "I can't wait to taste them myself," followed up by, "I really want to stick my cock in the twins' cunts." KISOR then told the UC, "and put it in 'Child 3's' ass."

12. On March 15, 2023, KISOR was again communicating with the UC, but believed he was speaking to "Child 4" and stated, "I would like to see you and ['Child 3'] sucking my cock." "Child 4" responded, "We never had a daddy at our parties before," and "I never suck a cock before, ['Child 3'] either." KISOR then responded, "and if you wanted me to, I would put my cock in your little pussies," "And assholes." "Child 4" asked, "will it hurt?" to which KISOR replied "not if I tongue it enough." Later in the same conversation, KISOR stated "did your

momma tell you I want to pierce your little nipples?" "Child 4" replied, "No. How come?" KISOR responded, "they look pretty for daddy and makes them super sensitive." "Child 4" then asked, "What's that mean?" to which KISOR replied, "that means you could cum by me just rubbing on your nipples." Then "Child 4" stated "Cum?" KISOR went on to make more sexually explicit comments later in the conversation to "Child 4," stating, "would you like to fuck daddy?" "How about ['Child 3']? Would she like to have daddy fuck her?" and "You can bounce up and down on daddy's cock." The text conversation continued in this manner with KISOR giving sexually explicit instructions on how to perform sexual acts to "Child 4".

13. In a text message conversation occurring on March 17, 2023, the UC asked KISOR about being released early from probation, KISOR responded "the chances would be pretty good with all the positive reviews I am getting now." KISOR immediately followed that statement up with "how are my little fuck toys tonight?" in referring to the UC's notional children. KISOR proceeded to express his desire to watch and participate in sexual acts with the UC's notional children making statements "I would love to see them fist their sisters." In this statement KISOR is referring to "Child 3" and "Child 4" who he believes are eight (8) years old.

14. KISOR continued to communicate with the UC over the course of the next several months, in a similar manner. On January 11, 2024, KISOR texted the UC and asked if he could call her and speak to her on the phone. The UC stated "can we just talk for a bit (meaning text) and not be so pushy. I mean are you even out of that house place yet?" The UC was referring to the halfway house (Alvis house) that KISOR was residing at upon his release from prison. KISOR responded "I have been home about 3 months now." Later in the text messaging conversation KISOR stated "I got some new toys," and asked, "want me to show you?" followed by "is any of

the girls there?" KISOR also asked the UC "Would you like to see the twins together on the double headed one?"

15. On January 25, 2024, KISOR called the UC and they spoke on the phone. During the conversation the UC stated "I know. It's been a while. But I guess I'm just kind of wondering where we're at like, and you know, how much risk I want to take considering, you know, you just got out of jail again and I'm sure people are paying attention to what you're doing and trying to keep an eye on you." KISOR responded "The only person keeping an eye on me right now is my parole officer and he comes down every so often and that's one reason why I will not get a smartphone because they can put monitoring software on it, but as long as I have my little flip phone right now, he ain't got a problem with it." KISOR then discussed how he wanted to work on his mobile home for the UC and her children to live in when they arrived.

16. During the same conversation the UC asked KISOR "What kind of visit are you looking for? Because if we did do it, I mean their spring breaks got to be somewhere in March or April. It's usually around Easter time, I'll have to look. But you know, I never surprise the girls either and I never force them to do anything they don't want to do, so if that's where we're going." KISOR replied "It's whatever you all want to do. If they want to do something that's on them." KISOR then said, "Am I going to accommodate them? Absolutely." The UC replied "Okay. So if they're up for sex you're in for sex too." KISOR replied "Yes, if they're up… If you're up for it." KISOR also said, "So like I said, if we become a family unit, I'm going to be wore out. I won't have time to get on the computer. Except maybe to check emails." In that statement KISOR was referring to being physically exhausted from the sexual activity he will be engaged in with the UC and her notional children and not having the desire to look at illicit images on his computer.

17. Over the course of the next few months the communications between KISOR and the UC were intermittent as KISOR had begun employment. March 5, 2024, the UC texted KISOR, "So I guess you moved on because I won't always answer the phone even though I always been like this. Sorry." KISOR responded, "I haven't moved nowhere babe. I was severely sick and then got back to work." On March 29, 2024, KISOR texted the UC stating, "Hey babe, just wanted to let you know that I am back working at my old job that I had before my last driving job so if I don't text that much, that is the reason."

18. On March 5, 2024, KISOR reaffirmed his desire to have the UC and all of her notional children move to his home in Ohio and live with him, with KISOR implying he would like to help the UC financially once he is back to working full time again. In this conversation the UC stated, "No you said, a few minutes ago 'if you guys just came out here and we never did anything that's all I want, I want a family.' Now let's be honest if we came out there…" KISOR replied "I mean don't get me wrong I may be 56 years old, and it may not work as well as it did when I was in my thirties but that does not mean that I don't have a very talented tongue."

19. On April 12, 2024, KISOR texted the UC "This is the address to where i am going to live. After i get some cash saved up, i could see us buying a double-wide or a modular. 25630 canal rd. Circleville, Ohio 43113. Check it out on google maps." KISOR also asked, "Do you also think that all the girls would come? [Child 1] is an adult and capable of living on her own if she wanted too. I know i would love to be with all of you." The UC replied, "I will check it out a little later. I don't know if [Child 1] would come. She has a lot of friends here and a job."

20. On April 15, 2024, KISOR texted the UC the following messages "I cannot wait to see my cock sliding into [Child 3] and [Child 4]'s tight little twats." "I really do hope that [Child 1] comes because I promised her a good hard fucking a long time ago and i intend on delivering

in both her tight cunt and asshole. And [Child 2], i want to dump as many loads of cum in her as i can."

21. On July 30, 2024, KISOR demonstrated he still wanted the UC and her notional children to relocate to Ohio. KISOR asked the UC via text message, "Okay sweetheart, I want to know your thoughts about Ohio. Do you think it is possible?" "Have you asked the girls what they think about moving?" The UC replied "[Child 2] and the twins pretty much do what I want and ok with it. Honestly, don't think [Child 1] would come along. Not at first anyways."

22. On July 31, 2024, during a phone conversation, KISOR made the following statements to who he believed was the UC's Child 2.

- "Just understand one thing [Child 2], yes, I want to have sex with all of you." "you're gonna get your turn, I promise you that."
- "You want it in every hole don't ya?" "I'm going to have sex with all the girls, and you're ok with that."
- "I know your mom shows you pictures of my toys, you know I'm gonna use them on you."
- "and trust me, I have a very talented tongue, and I can't wait to eat your pussy."
- "I'd love to be playing with your boobs right now, and your pussy."

KISOR also told the UC he wanted to give it a few more months before the UC and her children come to stay with him. KISOR also made statements during the conversation that he isn't supposed to leave the state, but he would. He also stated, "I'm going to have sex with all the girls, and you're ok with that."

23. On September 30, 2024, the UC texted KISOR, "if you are still in this with us let me know. I think I am going to plan for week of Oct21. They have a day off school the week before

but my boss asked I not go then as it is long weekend for travelers." KISOR replied "I am so ready to meet you and the girls. Can you give me a call?"

24. On October 4, 2024, KISOR made the following statements to the UC via phone conversation. "I was in prison twice for what we're going to do." "I am so looking forward to seeing you and the girls." During the conversation KISOR discussed his plans to assume the mortgage on his deceased father's home with the UC and stated his intention to have a home for all of them (UC and children) to live together.

25. On October 10, 2024, the UC texted KISOR "Finally told [Child 2] my plans for next few weeks for sure. She was like well what do we do while you with daddy?" KISOR replied to the UC "She can be entertained by my tongue when I am done with you. I just can't wait to have you and the girls in my arms."

26. Over several months, KISOR has repeatedly discussed with the UC his desire to have her (UC) and her notional children come and live with him at his current address of 25630 Canal Rd., Circleville, OH 43113. KISOR has also communicated over approximately 21 months via email, text messaging, and phone calls his desire to have an open relationship with the UC and her notional daughters. KISOR has repeatedly made sexually explicit statements to the UC indicating his intentions to perform sex acts on the UC's notional daughters whom he (KISOR) believes are minors aged fourteen (14) and eight (8) years old.

27. On November 4, 2024, via text message, the UC and KISOR discuss KISOR bringing a gift for the UC's notional daughters when they meet. KISOR asks the UC "what would Sarah's measurements be?" "And also, the twins." On November 5, 2024, the UC replies to KISOR's previous text message stating "Off to work but she is 34b, size 6 womens so small woman. Twins are a large in girls. So like 14."

28. On November 6, 2024, KISOR replies to the UC via text message "I found some sexy silk bikini panties and top for twins and silk panties and bra with garter belt and stockings for Sarah. May order Saturday. Early Christmas present for them."

29. On November 7, 2024, KISOR via text message to the UC but addressing "Child 2" states "Dear [Child 2], I want you and your sisters to know this: I can't wait until I hold you in my arms and make sweet love to you in all of your holes and feel your lips on my dick. I want to make your pussy, asshole, mouth, and throat mine." KISOR then sent another text message addressing "Child 3" and "Child 4" stating "Dear [Child 3] and [Child 4], I can't wait to hold you in my arms and teach you both the pleasure of sex. I want to feel my cock sliding in and out of all your holes."

30. On November 13, 2024, Kisor sent the UC a text message stating "Good morning sweetheart, I pray for safe travels for you and the girls today. I can't wait for the girls to model the outfits I ordered for them." KISOR then tells the UC "Moms' tablet is also where pictures of the girls outfits are. KISOR "I just ordered them last night babe. Hopefully will be here before you and the girls go back to Colorado." KISOR made statements previously to the UC that he was going to order "outfits' for the UC's notional girls to wear for him.

31. On November 14, 2024, KISOR sent a text message to the UC stating "Good morning beautiful, I hope that you and the girl slept well. Please be careful driving here today because it has been raining bad and the roads are quite slick. Love you Bunches!" KISOR stated to the UC "I am working and will get off at 3:30p.m. Would you want to come by the house before you go to hotel." The UC replies "Prob just go to hotel cuz we went to get showered and dressed up for you."

32. The UC then told KISOR "Hey love My boss confirmed a room at the Hampton inn at 700 Canal st in canal Winchester. We will be there in about 15 mins. Holy fuck this is real now. Cant wait til you get here. Tell us when you leave." KISOR responded "Where is here? Let me know place and room number(s). okay?" KISOR then asks "What room number?", and "I see the building. Can you meet me outside?"

33. On November 14, 2024, at approximately 4:10 p.m., KISOR arrived at the Hampton Inn hotel located at 700 W Waterloo St., Canal Winchester, OH. KISOR circled the parking lot once slowly and then pulled into a parking spot in the front of the hotel. It was at that time that HSI Special Agents took KISOR into custody without incident.

34. On November 13, 2024, KISOR stated to the UC, "I have my moms tablet which has Bluetooth capability." KISOR stated "Moms' tablet is also where pictures of the girls' outfits are." KISOR's mother passed away earlier in the year, and that is how he came into possession of the tablet. KISOR has previously stated he has a home computer as well as the tablet. The tablet was not located on KISOR or in his vehicle, it is believed the tablet is at KISOR's personal residence.

DEFINITIONS

35. The following definitions apply to this Affidavit and Attachment B:

a. "Chat," as used herein, refers to any kind of text communication over the Internet that is transmitted in real-time from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

b. "Child erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily obscene or do not necessarily depict minors engaging in sexually explicit conduct.

c. "Child pornography," as defined in 18 U.S.C. § 2256(8), is any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical or other means, of sexually explicit conduct, where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

d. "Cloud storage," as used herein, is a form of digital data storage in which the digital data is stored on remote servers hosted by a third party (as opposed to, for example, on a user's computer or other local storage device) and is made available to users over a network, typically the Internet.

e. "Computer," as used herein, refers to "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device" and includes smartphones, other mobile phones, and other mobile devices. *See* 18 U.S.C. § 1030(e)(1).

f. "Computer hardware," as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing

devices (including central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, "thumb," "jump," or "flash" drives, which are small devices that are plugged into a port on the computer, and other memory storage devices); peripheral input/output devices (including keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).

g. "Computer passwords and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

h. "Computer-related documentation," as used herein, consists of written, recorded, printed, or electronically stored material that explains or illustrates how to configure or use computer hardware, computer software, or other related items.

i. "Computer software," as used herein, is digital information that can be interpreted by a computer and any of its related components to direct the way it works. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

j. A provider of "Electronic Communication Service" ("ESP"), as defined in 18 U.S.C. § 2510(15), is any service that provides to users thereof the ability to send or receive wire or electronic communications. For example, "telephone companies and electronic mail companies" generally act as providers of electronic communication services. See S. Rep. No. 99-541 (1986), reprinted in 1986 U.S.C.C.A.N. 3555, 3568.

k. The "Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

l. "Internet Service Providers" ("ISPs"), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, email, remote storage, and co-location of computers and other communications equipment.

m. An "Internet Protocol address" or "IP address," as used herein, refers to a unique numeric or alphanumeric string used by a computer or other digital device to access the Internet. Every computer or device accessing the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer or device may be directed properly from its source to its destination. Most Internet Service Providers ("ISPs") control a range of IP addresses. IP addresses can be "dynamic," meaning that the ISP assigns a different unique number to a computer or device every time it accesses the Internet. IP addresses might also be "static," if an ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet. ISPs typically maintain logs of the subscribers to whom IP addresses are assigned on particular dates and times.

n. "Minor," as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

o. "Mobile applications," as used herein, are small, specialized programs downloaded onto mobile devices that enable users to perform a variety of functions, including engaging in online chat, reading a book, or playing a game.

p. "Records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

q. "Remote computing service," as defined in 18 U.S.C. § 2711(2), is the provision to the public of computer storage or processing services by means of an electronic communications system.

r. "Sexually explicit conduct," as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the anus, genitals, or pubic area of any person.

s. "Short Message Service" ("SMS"), as used herein, is a service used to send text messages to mobile phones. SMS is also often referred to as texting, sending text messages or text messaging. The service allows for short text messages to be sent from one cell phone to another cell phone or from the Web to another cell phone.

t. A "storage medium" is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, "thumb," "jump," or "flash" drives, CD-ROMs, and other magnetic or optical media.

u. "URL" is an abbreviation for Uniform Resource Locator and is another name for a web address. URLs are made of letters, numbers, and other symbols in a standard form. People use them on computers by clicking a pre-prepared link or typing or copying and pasting one into a web browser to make the computer fetch and show some specific resource (usually a web page) from another computer (web server) on the Internet.

v. "Visual depiction," as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

BACKGROUND ON OBSCENE MATERIAL OF CHILDREN, CHILD PORNOGRAPHY, COMPUTERS, AND THE INTERNET

36. I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience, and knowledge, I know the following:

a. Computers and digital technology are the primary way in which individuals interested in child pornography interact with each other. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

b. Digital cameras and smartphones with cameras save photographs or videos as a digital file that can be directly transferred to a computer by connecting the camera or smartphone to the computer, using a cable or via wireless connections such as "WiFi" or "Bluetooth." Photos and videos taken on a digital camera or smartphone may be stored on a removable memory card in the camera or smartphone. These memory cards are often large enough to store thousands of high-resolution photographs or videos.

c. A modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Mobile devices such as smartphones and tablet

computers may also connect to other computers via wireless connections. Electronic contact can be made to literally millions of computers around the world. Child pornography can therefore be easily, inexpensively, and anonymously (through electronic communications) produced, distributed, and received by anyone with access to a computer or smartphone.

d. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. Electronic storage media of various types—to include computer hard drives, external hard drives, CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small devices that are plugged into a port on the computer—can store thousands of images or videos at very high resolution. It is extremely easy for an individual to take a photo or a video with a digital camera or camera-bearing smartphone, upload that photo or video to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices. Some media storage devices can easily be concealed and carried on an individual's person. Smartphones and/or mobile phones are also often carried on an individual's person.

e. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

f. Individuals also use online resources to retrieve and store child pornography. Some online services allow a user to set up an account with a remote computing service that may provide email services and/or electronic storage of computer files in any variety of formats. A user can set up an online storage account (sometimes referred to as "cloud" storage) from any computer or smartphone with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer, smartphone, or external media in most cases.

g. A growing phenomenon related to smartphones and other mobile computing devices is the use of mobile applications, also referred to as "apps." Apps consist of software downloaded onto mobile devices that enable users to perform a variety of tasks – such as engaging in online chat, sharing digital files, reading a book, or playing a game – on a mobile device. Individuals commonly use such apps to receive, store, distribute, and advertise child pornography, to interact directly with other like-minded offenders or with potential minor victims, and to access cloud-storage services where child pornography may be stored.

h. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional (*i.e.*, by saving an email as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files) or unintentional. Digital information, such as the traces of the path of an electronic communication, may also be automatically stored in many places (*e.g.*, temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

CHARACTERISTICS COMMON TO INDIVIDUALS WHO HAVE A SEXUAL INTEREST IN CHILDREN OR WHO SOLICIT CHILD PORNOGRAPHY

37. Based on my previous investigative experience related to child-exploitation investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who have a sexual interest in children and/or solicit child pornography:

a. Such individuals may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged

in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity.

b. Such individuals may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Such individuals almost always possess and maintain child pornographic material in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain those materials and child erotica for many years.

d. Likewise, such individuals often maintain their child pornography images in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These child pornography images are often maintained for several years and are kept close by, usually at the possessor's residence, inside the possessor's vehicle, or, at times, on their person, or in cloud-based online storage, to enable the individual to view the child pornography images, which are valued highly. Some of these individuals also have been found to download, view, and then delete child pornography on their computers or digital devices on a cyclical and repetitive basis.

e. Importantly, evidence of such activity, including deleted child pornography, often can be located on these individuals' computers and digital devices through the use of forensic

tools. Indeed, the very nature of electronic storage means that evidence of the crime is often still discoverable for extended periods of time even after the individual "deleted" it.1

f. Such individuals also may correspond with and/or meet others to share information and materials, rarely destroy correspondence from other child pornography distributors/possessors, conceal such correspondence as they do their sexually explicit material, and often maintain contact information (e.g., online messaging accounts, email addresses, etc.) of individuals with whom they have contacted and who share the same interests in child pornography.

g. Such individuals prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

h. Even though an individual uses a portable device to access the Internet and obscene material of children child pornography, it is more likely than not that evidence of this access will be found on electronic storage devices in the possession of the individual, as set forth in Attachment A, including on digital devices other than the portable device (for reasons including the frequency of "backing up" or "synching" mobile phones to computers or other digital devices).

38. Based on all of the information contained herein, I believe that a Jason J. ATHA likely displays characteristics common to individuals who have a sexual interest in children and/or solicits obscene material of children and child pornography.

---

1 *See United States v. Carroll*, 750 F.3d 700, 706 (7th Cir. 2014) (concluding that 5-year delay was not too long because "staleness inquiry must be grounded in an understanding of both the behavior of child pornography collectors and of modern technology"); *see also United States v. Seiver*, 692 F.3d 774 (7th Cir. 2012) (Posner, J.) (collecting cases, e.g., *United States v. Allen*, 625 F.3d 830, 843 (5th Cir. 2010); *United States v. Richardson*, 607 F.3d 357, 370-71 (4th Cir. 2010); *United States v. Lewis*, 605 F.3d 395, 402 (6th Cir. 2010)).

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

39. As described above and in Attachment B, this application seeks permission to search for records that might be found in electronic storage devices found on the person of KISOR, in whatever form they are found. One form in which the records are likely to be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

40. I submit that if a computer or storage medium is found on KISOR, described in Attachment A, there is probable cause to believe those records referenced above will be stored on that computer or storage medium, for at least the following reasons:

a. Deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

b. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has

been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

41. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in electronic storage devices on the person of KISOR because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, email programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files

were created and the sequence in which they were created, although this information can later be falsified.

b. Information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (*e.g.*, registry information, communications, images and movies, transactional information, records of session times and durations, Internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, computers typically contain information that logs: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the Internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data

typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (*e.g.*, a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (*e.g.*, Internet searches indicating criminal planning), or consciousness of guilt (*e.g.*, running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not

present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f. I know that when an individual uses a computer to obtain or access obscene material, child pornography or solicit a minor for sex, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

42. Based upon my training and experience and information relayed to me by agents and others involved in the forensic examination of computers, I know that computer data can be stored on a variety of systems and storage devices, including external hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, cellular phones capable of storage. I also know that during the search of the electronic storage devices on the person, it is not always possible to search computer equipment and storage devices for data for a number of reasons, including the following:

a. Searching computer systems is a highly technical process that requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is impossible to bring to the search website all of the technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer,

software, or operating system that is being searched;

b. Searching computer systems requires the use of precise, scientific procedures which are designed to maintain the integrity of the evidence and to recover "hidden," erased, compressed, encrypted, or password-protected data. Computer hardware and storage devices may contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Since computer data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is essential to conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted;

c. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises; and

d. Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Computer users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. In addition, computer users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography a computer user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is contraband, evidence, fruits,

or instrumentalities of a crime.

43. Additionally, based upon my training and experience and information relayed to me by agents and others involved in the forensic examination of computers, I know that routers, modems, and network equipment used to connect computers to the Internet often provide valuable evidence of, and are instrumentalities of, a crime. This is equally true of wireless routers, which create localized networks that allow individuals to connect to the Internet wirelessly. Though wireless networks may be secured (in that they require an individual to enter an alphanumeric key or password before gaining access to the network) or unsecured (in that an individual may access the wireless network without a key or password), wireless routers for both secured and unsecured wireless networks may yield significant evidence of, or serve as instrumentalities of, a crime—including, for example, serving as the instrument through which the perpetrator of the Internet-based crime connected to the Internet and, potentially, containing logging information regarding the time and date of a perpetrator's network activity as well as identifying information for the specific device(s) the perpetrator used to access the network. Moreover, I know that individuals who have set up either a secured or unsecured wireless network in their residence are often among the primary users of that wireless network.

44. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

SEARCH METHODOLOGY TO BE EMPLOYED

45. The search procedure of electronic data contained in computer hardware, computer software, smartphone storage and/or memory storage devices may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):

a. on-site triage of computer systems (laptops, desktops, etc.) and/or mobile devices (smart phones, tablets, etc.) to determine what, if any, peripheral devices or digital storage units have been connected to such computer systems, as well as a preliminary scan of image files contained on such systems and digital storage devices to help identify any other relevant evidence or potential victims;

b. examination of all of the data contained in such computer hardware, computer software, or memory storage devices to view the data and determine whether that data falls within the items to be seized as set forth herein;

c. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);

d. surveying various file directories and the individual files they contain;

e. opening files in order to determine their contents;

f. scanning storage areas;

g. performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment B; and

h. performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment B.

DEVICES WITH BIOMETRIC SECURITY FEATURES

46. The warrant I am applying for would permit law enforcement to obtain from certain individuals the display of physical biometric characteristics (such as fingerprint, thumbprint, or facial characteristics) in order to unlock computers and mobile devices (digital devices), and mobile applications within the mobile devices, subject to search and seizure pursuant to this warrant. I seek this authority based on the following:

a. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many digital devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the digital devices through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners and facial recognition features. Some digital devices offer a combination of these biometric features, and the user of such digital devices can select which features they would like to utilize.

b. If a digital device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called “Touch ID,” which allows a user to register up to five fingerprints that can unlock a digital device. Once a fingerprint is registered, a user can unlock the digital device by pressing the relevant finger to the digital device’s Touch ID sensor, which is found in the round button (often referred

to as the "home" button) located at the bottom center of the front of the digital device. The fingerprint sensors found on digital device produced by other manufacturers have different names but operate similarly to Touch ID.

c. If a computer is equipped with a facial recognition feature, a user may enable the ability to unlock the digital device and applications through his or her face. For example, Apple offers a facial recognition feature called "Face ID." During the Face ID registration process, the user holds the digital device in front of his or her face. The digital device's camera then analyzes and records data based on the user's facial characteristics. The digital device and applications can then be unlocked if the camera detects a face with characteristics that match those of the registered face. Facial recognition features found on digital device's produced by other manufacturers have different names but operate similarly to Face ID.

d. In my training and experience, users of digital device often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a digital device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a digital device's contents. This is particularly true when the users of a computer are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

e. As discussed in this affidavit, based on my training and experience I believe that one or more digital devices will be found during the search. The passcode or password that would unlock the digital devices and/or mobile applications within the device subject to search under this warrant is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the digital devices, making the use of biometric features necessary to the execution of the search authorized by this warrant.

f. I also know from my training and experience, as well as from information found in publicly available materials including those published by digital device manufacturers, that biometric features will not unlock a computer in some circumstances even if such features are enabled. This can occur when a computer has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when (1) more than 48 hours has elapsed since the device was last unlocked or (2) when the device has not been unlocked using a fingerprint for 4 hours and the passcode or password has not been entered in the last 16 hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked computer equipped with biometric features, the opportunity to unlock the digital devices through a biometric feature may exist for only a short time.

g. In my training and experience, the person who is in possession of a digital device or has the digital device among his or her belongings at the time the computer is found is likely a user of the digital device. However, in my training and experience, that person may not be the only user of the digital device whose physical characteristics are among those that will unlock the digital device via biometric features, and it is also possible that the person in whose possession the digital device is found is not actually a user of that digital device at all. Furthermore, in my training and experience, I know that in some cases it may not be possible to know with certainty who is the user of a given digital device, such as if the digital device is found in a common area of a residence without any identifying information on the exterior of the device. Nevertheless, law enforcement is seeking authority to require KISOR, to unlock any digital device reasonably believed to contain evidence of violations of 18 U.S.C. §§ 2422(b) and 2252A, by using biometric unlock features in the same manner as discussed above.

h. Due to the foregoing, if law enforcement personnel encounter a digital device that is subject to search and seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, the warrant I am applying for would permit law enforcement personnel to: (1) press or swipe the fingers (including thumbs) of KISOR, to the fingerprint scanner of the digital device; (2) hold the digital device in front of the face of KISOR and activate the facial recognition feature, for the purpose of attempting to unlock the digital device and applications in order to search its contents as authorized by this warrant.

CONCLUSION

47. Based on the aforementioned factual information, I respectfully submit that there is probable cause to believe that any computer(s), electronic mobile devices and electronic storage media found in the SUBJECT PREMISES, more specifically identified in Attachment A, contain evidence of a crime, contraband, fruits of a crime, or other items illegally possessed, or property designed for use, intended for use, or used in the commission of violations of 18 U.S.C. §§ 2422(b) and 2252A. I therefore respectfully request that the attached warrant be issued authorizing the search and seizure of the items listed in Attachment B.

Respectfully submitted,

E A La Vigne

Edward (Ted) La Vigne, Special Agent
Homeland Security Investigations

Sworn to before me and signed in my presence and/or by reliable electronic means,
per Fed.R.Crim.P. 4(d) and 4.1 on January 10, 2025.

Chelsey M. Vascura

Magistrate Judge Chelsey M. Vascura
United States District Court, Southern District of Ohio